We claim:

1. A method for tracing a sequence of packets to a potential source thereof within a communications network, the sequence of packets being received at a target host in said communications network at a received packet rate, the method comprising the steps of:

applying a burst load to each of one or more selected network elements in said communications network;

for each selected network element, measuring a change in said received packet rate in response to said application of said burst load to said selected network element; and

determining said potential source of said sequence of packets based on said measured changes in said received packet rate.

2. The method of claim 1 wherein said communications network comprises the Internet.

3. The method of claim 1 wherein each of said selected network elements comprises a network link.

4. The method of claim 3 wherein said step of applying a burst load to said network link comprises transmitting packets to a subnetwork of said communications network to initiate a responsive flow of packets through said network link.

5. The method of claim 4 wherein said transmitted packets are spoofed from an end of said network link closest to said target host.

6. The method of claim 4 wherein said transmitted packets comprise UDP chargen requests.

7. The method of claim 1 wherein each of said selected network elements comprises a network router.

8. The method of claim 1 further comprising the step of generating a map comprising routes from said target host to a plurality of subnetworks of said communications network.

9. The method of claim 1 further comprising the step of eliminating said selected network element from consideration as said potential source of said sequence of packets when said change in said received packet rate meets a predetermined criterion.

10. The method of claim 9 wherein said predetermined criterion comprises a determination of whether said change in said received packet rate is less than a predetermined threshold.

11. The method of claim 9 wherein said step of eliminating said selected network element from consideration also eliminates from consideration one or more subnetworks of said communications network which are connected to said selected network element.

12. The method of claim 1 wherein said sequence of packets comprises a Denial-of-Service attack on said target host.

13. The method of claim 1 wherein said steps of applying said burst load, measuring said changes in said received packet rate, and determining said potential source of said sequence of packets, are executed under the control of an automated algorithm.

14. The method of claim 1 wherein said steps of applying said burst load and determining said potential source of said sequence of packets, are executed under the at least partial control of a human operator.

15. The method of claim 14 further comprising the step of displaying information, said information including data representative of said measured changes in said received packet rate, to said human operator, for use by said human operator in exercising said at least partial control.

16. An apparatus for tracing a sequence of packets to a potential source thereof within a communications network, the sequence of packets being received at a target host in said communications network at a received packet rate, the apparatus comprising:

means for applying a burst load to each of one or more selected network elements in said communications network;

means for measuring changes in said received packet rate in response to said application of said burst load to each of said selected network elements; and

means for determining said potential source of said sequence of packets based on said measured changes in said received packet rate.

17. The apparatus of claim 16 wherein said communications network comprises the Internet.

18. The apparatus of claim 16 wherein each of said selected network elements comprises a network link.

19. The apparatus of claim 18 wherein said means for applying a burst load to said network link comprises means for transmitting packets to a subnetwork of said communications network to initiate a responsive flow of packets through said network link.

20. The apparatus of claim 19 wherein said transmitted packets are spoofed from an end of said network link closest to said target host.

21. The apparatus of claim 19 wherein said transmitted packets comprise UDP chargen requests.

22. The apparatus of claim 16 wherein each of said selected network elements comprises a network router.

23. The apparatus of claim 16 further comprising means for generating a map comprising routes from said target host to a plurality of subnetworks of said communications network.

24. The apparatus of claim 16 further comprising means for eliminating said selected network element from consideration as said potential source of said sequence of packets when said change in said received packet rate meets a predetermined criterion.

25. The apparatus of claim 24 wherein said predetermined criterion comprises a determination of whether said change in said received packet rate is less than a predetermined threshold.

26. The apparatus of claim 24 wherein said means for eliminating said selected network element from consideration also eliminates from consideration one or more subnetworks of said communications network which are connected to said selected network element.

27. The apparatus of claim 16 wherein said sequence of packets comprises a Denial-of-Service attack on said target host.

28. The apparatus of claim 16 wherein said means for applying said burst load, said means for measuring said changes in said received packet rate, and said means for determining said potential source of said sequence of packets, are executed under the control of an automated algorithm.

29. The apparatus of claim 16 wherein said means for applying said burst load and said means for determining said potential source of said sequence of packets are executed under the at least partial control of a human operator.

30. The apparatus of claim 29 further comprising means for displaying information, said information including data representative of said measured changes in said received packet rate, to said human operator, for use by said human operator in exercising said at least partial control.